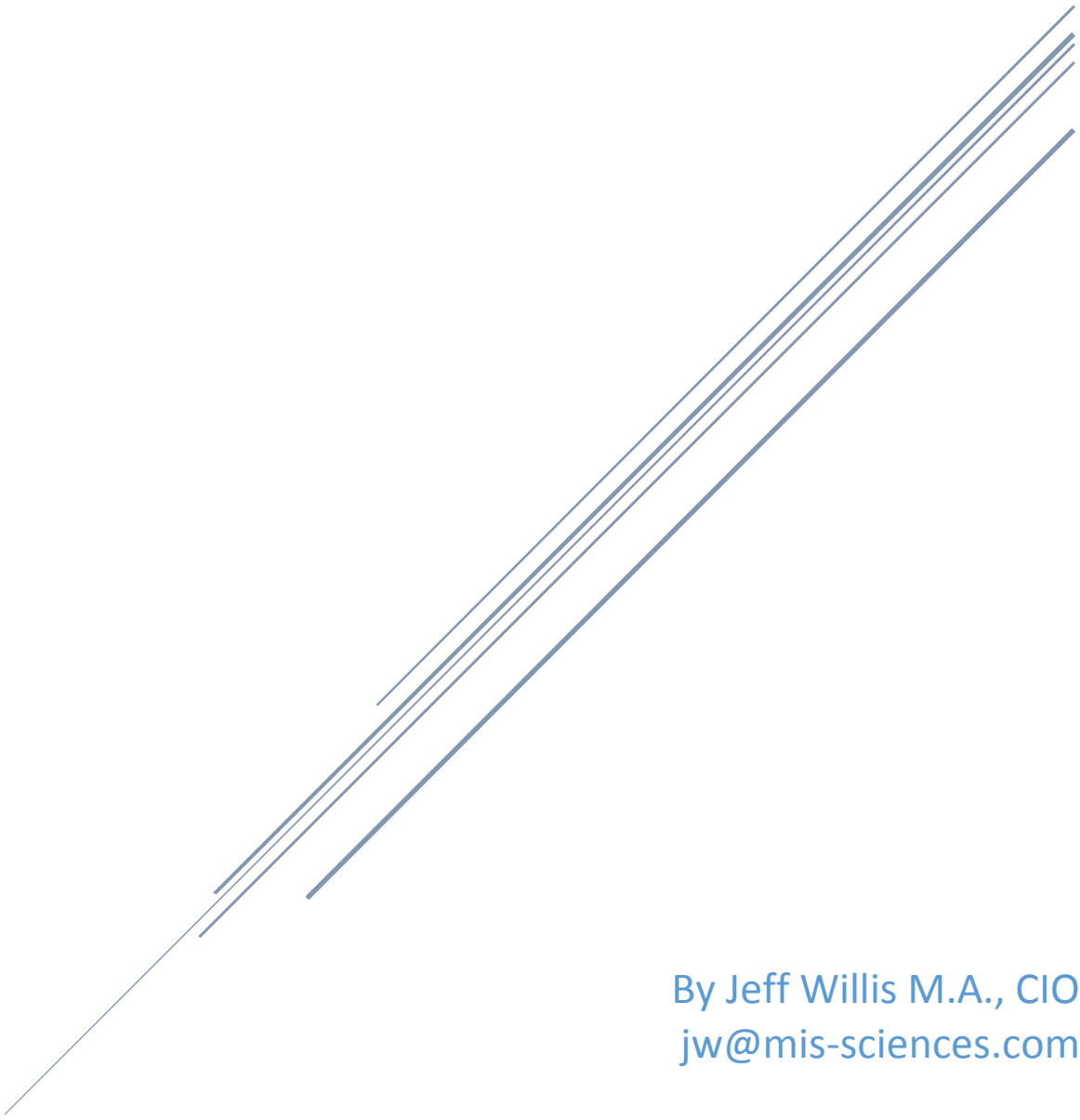
Disaster Recovery Site Considerations



By Jeff Willis M.A., CIO
jw@mis-sciences.com

Ver 1.3 - 20140416

GS-35F-0266S
SIN 132-51
SIN 132-52

Corporate Office
2550 North Hollywood Way
Suite 404
Burbank, CA 91505
1.818.847.0213
info@mis-sciences.com

Federal Services Office
1655 North Fort Myer Drive
Suite 700
Arlington, VA 22209
1.703.351.3366
fedinfo@mis-sciences.com

Las Vegas Office
322 Karen Ave
Suite 1407
Las Vegas, NV 89109
1.725.502.3755
lvinfo@mis-sciences.com

Disaster Recovery Site Considerations

Disaster recovery (DR) terminology can confuse -- terms like hot site, hybrid site, warm site and cold site are common in DR parlance and each has its own variances. Each option provides reliable disaster recovery, but which one is best suited for your corporate needs? Here's a look at the differences in disaster recovery and the pros and cons of each.

DR needs and site types will vary depending on recovery time objective (RTO), level of site complexity, data sensitivity and security requirements. The requirements for non-sensitive data for a small company will vary dramatically from those for a Government agency handling sensitive data where there are mandated security requirements and their sites are highly complex.

Hot DR Sites

Hot sites can come in many flavors: real-time hosted hot site; hosted hot site, and shared hot site. The type of hot site will be dictated by your RTO, complexity, and security requirements.

If the acceptable RTO for your company is a few hours instead of minutes and your security and complexity requirements are minimal, then a shared hot site is likely appropriate. The biggest difference between a shared hot site and a hosted hot site is the use of shared equipment for infrastructure components like servers and peripherals. Storage is dedicated and data replication is used to get data from the production site to the disaster recovery site. The method of data replication will vary depending on your RTO

Shared Hot DR Sites

Shared hot sites are less expensive than hosted sites because equipment in the DR facility is shared by multiple customers. Since DR service providers rely on the fact that not all customers have a disaster at the same time, the shared equipment is often a virtualized environment with each customer having their own guest machines and dedicated storage.

On the downside, using shared equipment is less flexible because customers are limited by the equipment the disaster recovery service provider offers. This limitation will often result in loss of certain functionality and may affect business operations, but will allow a business to remain operational until the man site can be fully recovered. While some service providers may have a limited selection of equipment, others are more flexible. Another consequence of using a site

with shared equipment is the time limit on how long customers can use the shared equipment if a disaster occurs. The limit varies among service providers, but typically ranges between 30 and 90 days. After this period, a customer must arrange to migrate to a cold site. This limitation is to prevent customers from turning a shared DR site into a permanent production site.

If there are special security and/or compliance requirements or highly complex environments, normally a Shared Hot Site should not be considered unless the DR provider can make special considerations that will not impact their other DR customers.

To avoid unpleasant surprises, a clear understanding of the terms, conditions and limitations of managed disaster recovery services is required prior to committing to an agreement that may span several years.

Hosted Hot DR Sites

Hosted hot sites are more expensive because they replicate your current environment from equipment, storage, network infrastructure, and security. The DR facility has an exact copy of your environment and once all data is synchronized, operation can continue indefinitely. Depending on the disaster, the DR facility could become the primary operational site and operate indefinitely.

The hosted hot site is normally replicated from the main site regularly, usually every 12-48 hours, and may not always contain real-time data or site updates. Data restoration from the most recent copy of the primary site backup is often required, to ensure the data is current.

Real-Time Hosted Hot DR Sites

This is identical to the Hosted Hot Site, except that data is replicated in real-time from the primary center to the DR center. This allows for almost instant recovery from a disaster without loss of data. Depending on the configuration, failover from the primary site to the DR site can automated when a failure is detected.

Depending on the network infrastructure and the replication methods, a real-time hosted hot DR site can also be used and a GEO load balanced site allow 100% uptime.

For security sensitive and/or sites with compliance requirements and complex sites where RTO must be kept at a minimum, the hosted DR site options are the recommended options.

Warm DR Sites

In contrast to a Hot DR Site, a Warm DR Site relies on backups for recovery. Warm DR Sites are similar to Hot DR Sites in that they can be Shared or Hosted, a decision dictated by the site and security requirements. The equipment is same as their HOT counterpart, except it sits idle until it is needed. Once the Warm DR Site is activated, recovery is performed and the site is activated.

In the past, there was a huge difference between Hot DR Sites and Warm DR Sites because backups were limited to tape. Warm DR Site RTO's were measured in days. Warm DR Sites that rely on tape-based backups for recovery are at the lower end of the DR services spectrum.

Tape recovery has questionable reliability since most backups are never performed with validation, due to time constraints. Tapes can become unreadable for many reasons or tape drives and libraries can and will "eat" tapes, rendering them useless. If recovering from tape for a Shared Warm DR site, it is incumbent that the DR provider can read your backup tapes. With the multitude of tape types and backup/recovery software types, tape recovery presents a "high risk". If tape is the chosen recovery method, the DR facility should be provided with a compatible tape library/drive and the software to ensure recovery. A good rule to follow is *Tapes should be used for archive purposes, not for production backup and recovery purposes.* Electronic vaulting of backup data, at multiple locations, should be considered as a more reliable option to tape backup.

Disk-based backups have narrowed the gap between warm sites and hot sites, and almost all disaster recovery service providers now offer an electronic vaulting option, which is essentially disk-based backup of production data over the network. RTOs and recovery point objectives (RPOs) of warm sites with electronic vaulting are typically less than a day, which is close to the recovery times offered by hot sites but at a fraction of the cost as opposed to Hot DR Sites. The biggest savings is in the replication process, and licenses. Electronic vaulting is closing the gap between tape-based recovery and a replicated DR infrastructure, and customers must look at it because of its price and reliability benefits.

The cost benefits of the Warm DR Site vs. the Hot DR Site will depend on the required infrastructure, security requirements, and business cost of "down time". With the advance in replication technology, often the price difference between a Hot DR Site and a Warm DR Site is negligible.

Cold DR Sites

A Cold DR Site is rented space with power, cooling and connectivity that's ready to accept equipment. If a business can tolerate a RTO of several weeks to many months, a cold site is an option for business processes that can be down for an extended period.

It's the customer's responsibility to provide equipment for the cold site during a disaster. A disaster recovery plan that relies on a cold site must clearly define procuring and delivering equipment to the cold site when a disaster strikes. It's a high risk strategy to rely on obtaining the equipment when it's needed as it may not be possible to get the equipment in a timely manner, or they may not be available at all.

Another risk factor is application and O/S software. In complex environments the software or versions used in the primary site may not be available for recovery in the DR site. Newer versions of software that may be available may cause compatibility issues with existing applications that must be recovered. If the available O/S and Applications are compatible, the risks are decreased and the RTO may also decrease.

When using a cold site, the rule of thumb is "we are starting over from the beginning". If your DR RTO strategy allows for this, then the Cold DR Site is an option to consider.

Cold DR Sites are not all negative. They are often used to complement hot sites and warm sites in case of disasters that last for an extended period. A cold site can serve as a contingency to migrate equipment from the HOT Shared DR Site or Warm DR Site to the cold site if a disaster lasts for an extended period. This allows time for equipment and software procurement, recovery, and testing. Migration from a HOT or Warm Shared DR site to the environment created in the Cold DR Space presents little risk and they are usually within the same facility and with current technology, site moves within the same facility present little or no down time.

With Governments or companies with special security and compliancy requirements, it is incumbent they fully understand the impact of a Cold DR Site on their operational requirements.

Once fully migrated to the Cold DR Site space, companies will often use this as their primary site since the capital investment has already been made and the applications and sites are serving the business as required. If used as the primary site, companies with special security and compliance requirements may require an audit of the new environment to ensure compliance.

About MIS Sciences Corporation

Since 1996, as a Woman Owned Small Business, MIS Sciences Corporation has been providing technology services to Government agencies and corporations.

MIS focuses on Managed Services and Hosting, Development and application management Services, DR Services, and Electronic Vaulting. MIS clients have access to over 60 data centers throughout the USA, Europe, Asia, and Australia.

As a GSA contractor, MIS has strong partner ties with other GSA contractors and can provide a total solution in a single package using various teaming contract vehicles.

MIS Intelligere Cloud Services provides Electronic Vaulting and backup services, CDN services, and GEO balanced managed services.

For further information:

Federal and GSA inquires:

Federal Services Office
1655 North Fort Myer Drive
Suite 700
Arlington, VA 22209
1.703.351.3366
fedinfo@mis-sciences.com

Non-Federal and Corporate Inquiries:

Corporate Office
2550 North Hollywood Way
Suite 404
Burbank, CA 91505
1.818.847.0213
info@mis-sciences.com

CTA, Teaming, SubK, JV, and Partnering Inquiries:

1.877.262.3923
partner@mis-sciences